Michigan

Office of the Auditor General

REPORT SUMMARY

Performance Audit

Enterprise Information Security Program

Department of Information Technology (DIT)

Report Number:
084-0581-06

Released:
April 2007

An enterprise information security program is the foundation of the State's security control structure and reflects management's commitment to address security risks. The Office of Enterprise Security (OES) is responsible for identifying, managing, and mitigating security risks and vulnerabilities. OES is charged with leading disaster recovery planning, risk management, and security awareness and training; working with State agencies on security issues; and enforcing State security policies.

Audit Objective:
To assess the effectiveness of DIT's efforts to fully implement an effective information security framework.

Audit Conclusion:
DIT's efforts to fully implement an effective information security framework were not effective. We noted four material conditions.

Material Conditions:
DIT had not fully developed its information security governance program (Finding 1). Also, DIT had not fully implemented a comprehensive enterprise information security framework (Finding 2). In addition, DIT did not ensure that the Michigan Information Technology Executive Council security subcommittee provided effective information security governance for the State (Finding 3). Further, DIT had not fully developed and implemented a comprehensive information security training program (Finding 4).

Noteworthy Accomplishments:
The State's chief information security officer was named Executive Alliance's Information Security Executive of the Year Central for 2006. The award recognizes individuals who have demonstrated outstanding leadership in the field of information security.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DIT's efforts to evaluate and manage the State's exposure to information security risks.

Audit Conclusion:
DIT's efforts to evaluate and manage the State's exposure to information security risks were moderately effective. Our assessment disclosed that DIT's enterprise information security risk management program included incident, threat, vulnerability, and emergency management practices as well as practices to restrict the State's end users from accessing high-risk or inappropriate Web sites. However, we noted three material conditions.

Material Conditions:
DIT had not fully implemented a comprehensive enterprise information security risk management program (Finding 5). Also, DIT needs to implement a more effective process for incorporating

security throughout an information system's system development life cycle (Finding 6). DIT had not established an integrated and comprehensive process to oversee and direct the State's disaster recovery planning efforts. In addition, DIT did not have fully documented and tested disaster recovery plans for critical enterprise systems and the State's infrastructure (Finding 7).

Noteworthy Accomplishments:
In 2003 and 2004, the State received National Association of State Chief Information Officers (NASCIO) recognition awards for security and emergency management. In 2003, the State won the award for the *Secure Michigan Initiative* project. The project included a rapid risk assessment to determine high-risk issues in relation to the security of the State's information technology (IT) infrastructure, policies, procedures, and systems.

In 2004, the State won the NASCIO award for the Michigan Critical Incident Management System (CIMS). During the August 2003 electrical blackout, DIT used CIMS to track and monitor data on the status of the State's critical infrastructure. Use of CIMS allowed DIT to quickly restore critical systems and desktop services in an orderly manner.

In February 2006, DIT participated in Cyber Storm, the first government-led cyber security exercise to examine the response, coordination, and recovery mechanisms to a simulated cyber event within international, federal, state, and local governments. The exercise simulated a sophisticated cyber attack through a series of scenarios directed against critical infrastructures.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DIT's efforts to evaluate and enforce compliance with information security policies and procedures.

Audit Conclusion:
DIT's efforts to evaluate and enforce compliance with information security policies and procedures were moderately effective. However, we noted two material conditions.

Material Conditions:
DIT did not sufficiently staff its internal audit function to effectively audit the State's IT environment. In addition, DIT did not coordinate with State agencies to ensure that sufficient IT audit resources were assigned to audit application controls for critical information systems (Finding 8). The Office of Enterprise Security had not fully developed and implemented performance metrics for critical components of its information security program (Finding 9).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:
Our audit report contains 9 findings and 11 corresponding recommendations. DIT's preliminary response indicates that it agrees with all of the recommendations and has complied or will comply with them.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

A copy of the full report can be
obtained by calling 517.334.8050
or by visiting our Web site at:
http://audgen.michigan.gov

Michigan Office of the Auditor General
201 N. Washington Square
Lansing, Michigan 48913

Thomas H. McTavish, C.P.A.
Auditor General

Scott M. Strong, C.P.A., C.I.A.
Deputy Auditor General